



# **Payment Card Industry (PCI) Data Security Standard**

---

## **Attestation of Compliance for Onsite Assessments – Merchants**

**Version 3.0**

February 2014

## Section 1: Assessment Information

### Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the merchant's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact your acquirer (merchant bank) or the payment brands for reporting and submission procedures.

### Part 1. Merchant and Qualified Security Assessor Information

#### Part 1a. Merchant Organization Information

Company Name:		DBA (doing business as):	
Contact Name:		Title:	
ISA Name(s) (if applicable):		Title:	
Telephone:		E-mail:	
Business Address:		City:	
State/Province:		Country:	
URL:		Zip:	

#### Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:			
Lead QSA Contact Name:		Title:	
Telephone:		E-mail:	
Business Address:		City:	
State/Province:		Country:	
URL:		Zip:	

### Part 2. Executive Summary

#### Part 2a. Type of Merchant Business (check all that apply)

- Retailer
  Telecommunication
  Grocery and Supermarkets  
 Petroleum
  E-Commerce
  Mail order/telephone order (MOTO)  
 Others (please specify):

What types of payment channels does your business serve?

- Mail order/telephone order (MOTO)  
 E-Commerce  
 Card-present (face-to-face)

Which payment channels are covered by this assessment?

- Mail order/telephone order (MOTO)  
 E-Commerce  
 Card-present (face-to-face)

**Note:** If your organization has a payment channel or process that is not covered by this assessment, consult your acquirer or payment brand about validation for the other channels.

### Part 2b. Description of Payment Card Business

How and in what capacity does your business store, process and/or transmit cardholder data?

### Part 2c. Locations

List types of facilities and a summary of locations included in PCI DSS review (for example, retail outlets, corporate offices, data centers, call centers, etc.)

Type of facility	Location(s) of facility (city, country)

### Part 2d. Payment Application

Does the organization use one or more Payment Applications?  Yes  No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	

### Part 2e. Description of Environment

Provide a **high-level** description of the environment covered by this assessment.

*For example:*

- *Connections into and out of the cardholder data environment (CDE).*
- *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*

Does your business use network segmentation to affect the scope of your PCI DSS environment?

*(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*

Yes

No

### Part 2f. Third-Party Service Providers

Does your company share cardholder data with any third-party service providers (for example, gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?

- Yes  
 No

**If Yes:**

Name of service provider:	Description of services provided:

**Note:** Requirement 12.8 applies to all entities in this list.

## Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input type="checkbox"/> No

## Section 3: Validation and Attestation Details

### Part 3. PCI DSS Validation

Based on the results noted in the ROC dated (*completion date*), the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document as of (*date*) (**check one**):

- Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby (*Merchant Company Name*) has demonstrated full compliance with the PCI DSS.
- Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby (*Merchant Company Name*) has not demonstrated full compliance with the PCI DSS.
- Target Date** for Compliance:
- An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with your acquirer or the payment brand(s) before completing Part 4.*
- Compliant but with Legal exception:** One or more requirements are marked “Not in Place” due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.
- If checked, complete the following:*
- | Affected Requirement | Details of how legal constraint prevents requirement being met |
|----------------------|--|
|                      |  |
|                      |  |

### Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(*Check all that apply*)

- The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version (*version number*), and was completed according to the instructions therein.
- All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
- I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
- I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
- If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

**Part 3a. Acknowledgement of Status (continued)**

- No evidence of full track data<sup>1</sup>, CAV2, CVC2, CID, or CVV2 data<sup>2</sup>, or PIN data<sup>3</sup> storage after transaction authorization was found on ANY system reviewed during this assessment.
- ASV scans are being completed by the PCI SSC Approved Scanning Vendor (*ASV Name*)

**Part 3b. Merchant Attestation**

<i>Signature of Merchant Executive Officer</i> ↑	<i>Date:</i>
<i>Merchant Executive Officer Name:</i>	<i>Title:</i>

**Part 3c. QSA Acknowledgement (if applicable)**

If a QSA was involved or assisted with this assessment, describe the role performed:	
--	--

<i>Signature of QSA</i> ↑	<i>Date:</i>
<i>QSA Name:</i>	<i>QSA Company:</i>

**Part 3d. ISA Acknowledgement (if applicable)**

If an ISA was involved or assisted with this assessment, describe the role performed:	
---	--

<i>Signature of ISA</i> ↑	<i>Date:</i>
<i>ISA Name:</i>	<i>Title:</i>

<sup>1</sup> Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

<sup>2</sup> The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

<sup>3</sup> Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

## Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement. If you answer “No” to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

*Check with your acquirer or the payment brand(s) before completing Part 4.*

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If “NO” selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input type="checkbox"/>	<input type="checkbox"/>	

